DEVINITI

GenAI
Practitioners' Hub

Kara
**Herbut**

# Building AI Agents Right

## How to avoid common project failures

26 FEB 2025

# Building AI Agents is very hard

# Agenda

- What is AI agent and do you need one?
- Why AI Agent projects fail
- Common mistakes to avoid
- How to set your project up for success

**Housekeeping**

- Webinar will last around 30 minutes (+ 10min for Q&A)
- Feel free to ask questions anytime via dedicated ‘Questions’ feature

# What are AI Agents?

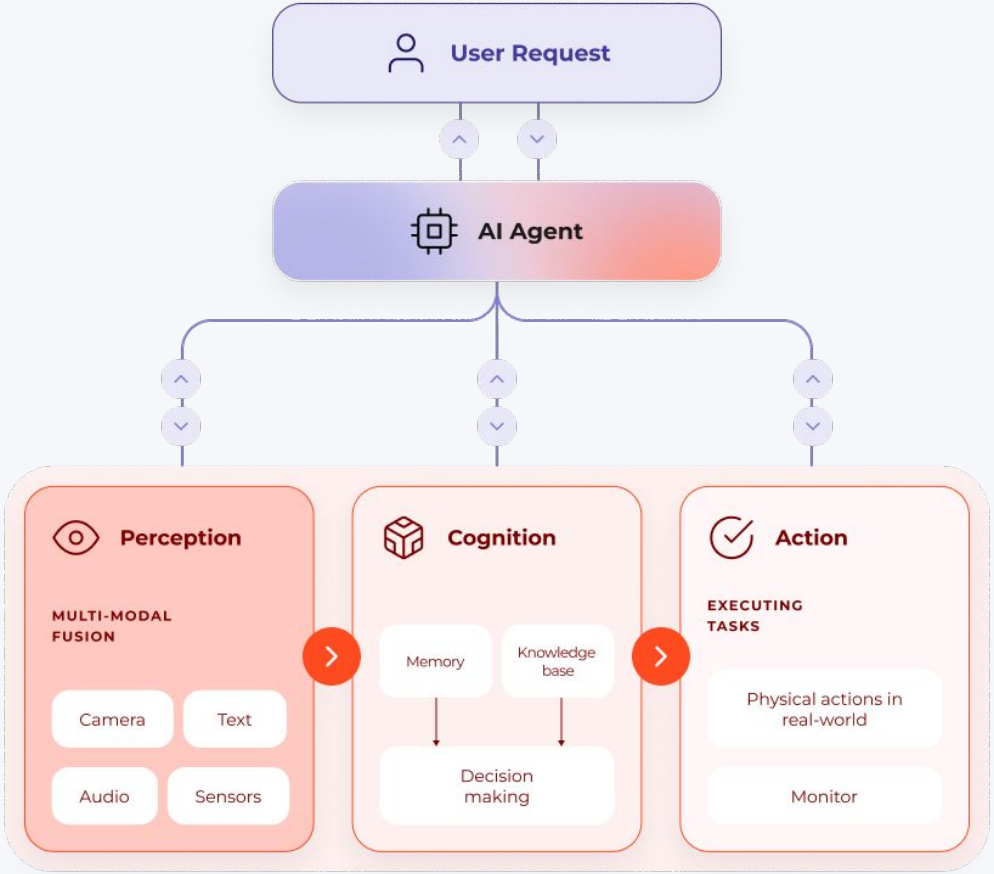
“Agents are **fully autonomous** systems that operate independently over **extended periods**, using various tools to accomplish **complex tasks.**.”

Source: Antropic https://www.anthropic.com/research/building-effective-agents

“Agents are programs where **LLM outputs control the workflow”**

Source:https://huggingface.co/docs/smolagents/en/conceptual_guides/intro_agents

# AI Agent


User Request
AI Agent
Perception
MULTI-MODAL FUSION
Camera
Text
Audio
Sensors
Cognition
Memory
Knowledge base
Decision making
Action
EXECUTING TASKS
Physical actions in real-world
Monitor

# Deterministic vs non-deterministic software

“One of the inherent characteristics of GenAI is its **non-determinism**. This means the AI can produce different outputs even when given the same input multiple times, leading to unpredictability in its results.”

Gonçalo Ribeiro, CEO of YData.

# Do you need an AI Agent?

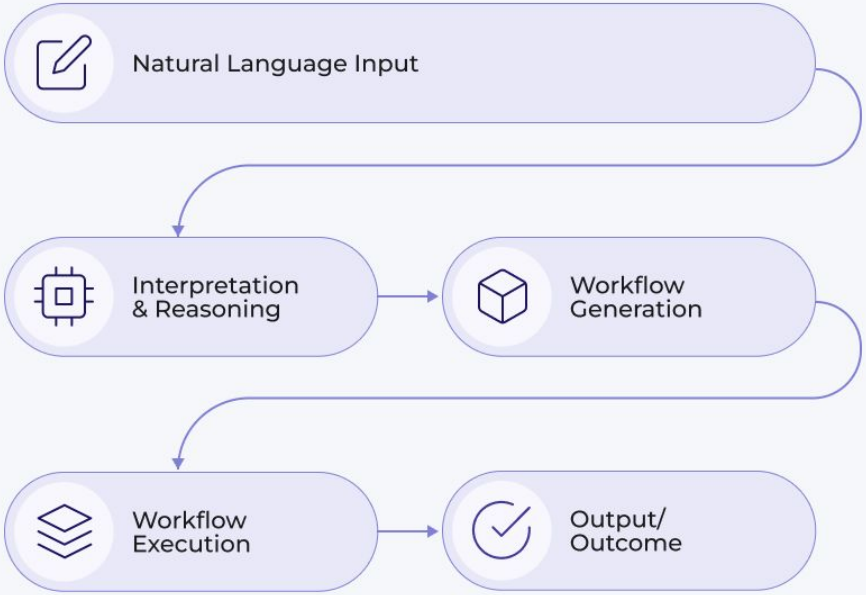
“When building applications with LLMs, we recommend finding the simplest solution possible [...]. **This might mean not building agentic systems at all.”**

Source: Anthropic

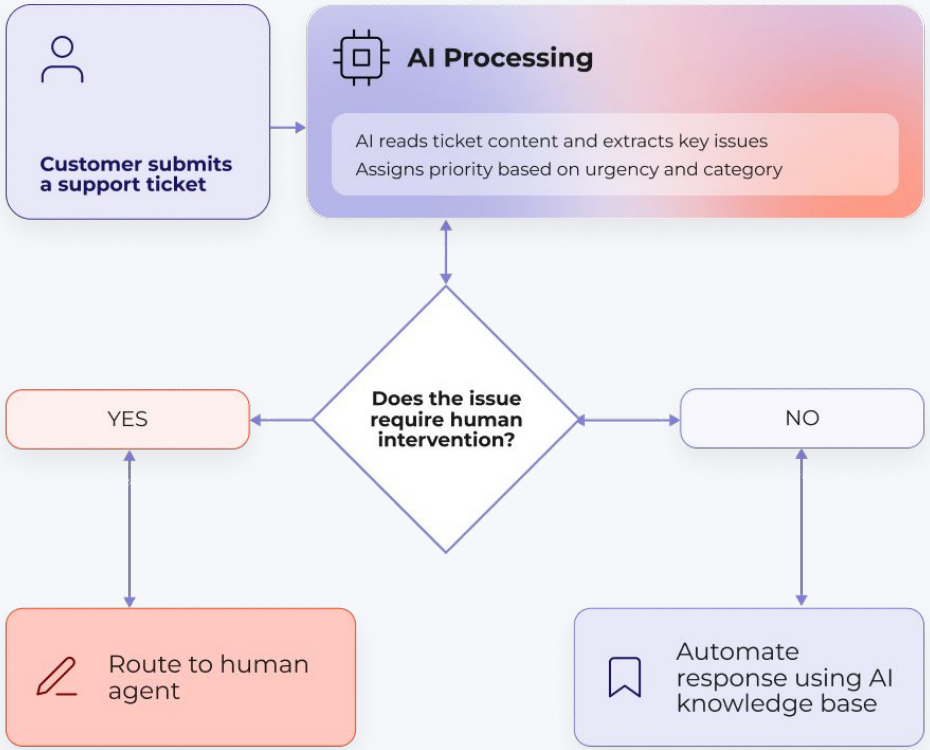
# Automation vs AI Workflows vs AI Agents

| | Automation | AI Workflows | AI Agents |
|---|---|---|---|
| **What is does** | Fixed, rule-based tasks | Execute predefined sequences of tasks. | Operate autonomously with the ability to adapt to changing environments. |
| **Ideal use case** | For predictive repetitive processes without human intervention | Processes that are well understood and can be broken down into separate steps. | Unpredictable environments where complex decision-making and learning from interactions is needed |
| **Example** | Automatically sending email confirmations after purchase | Automating data entry from emails into a database using a series of rule-based steps. | A virtual customer service representative that understands natural language, responds to diverse queries, and improves its responses over time. |

# AI Workflows



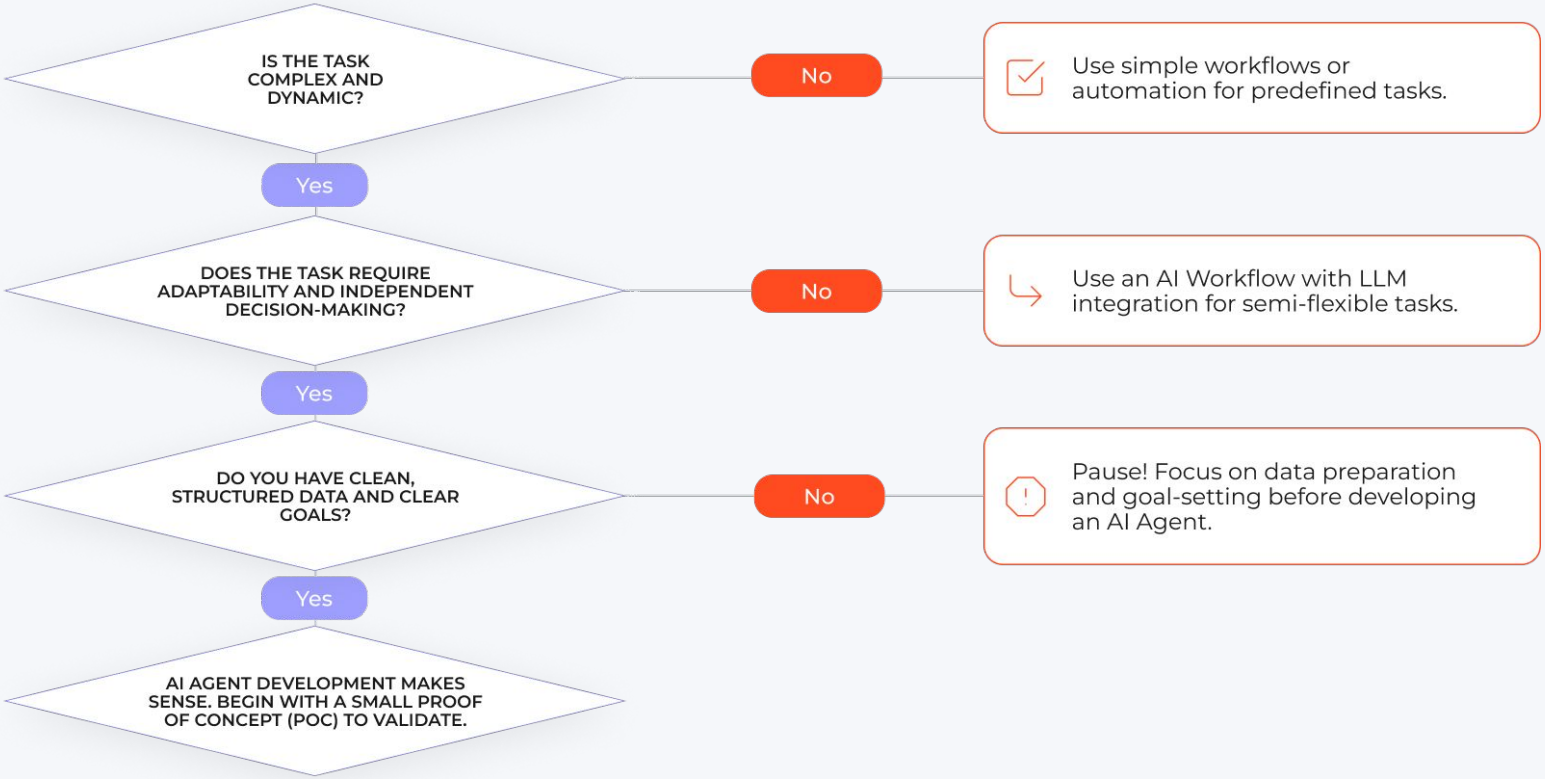
# AI Workflow example



# Automation vs AI Workflows vs AI Agents

| | Automation | AI Workflows | AI Agents |
|---|---|---|---|
| **What is does** | Fixed, rule-based tasks | Execute predefined sequences of tasks. | Operate autonomously with the ability to adapt to changing environments. |
| **Ideal use case** | For predictive repetitive processes without human intervention | Processes that are well understood and can be broken down into separate steps. | Unpredictable environments where complex decision-making and learning from interactions is needed |
| **Example** | Automatically sending email confirmations after purchase | Automating data entry from emails into a database using a series of rule-based steps. | A virtual customer service representative that understands natural language, responds to diverse queries, and improves its responses over time. |

# Do you need an AI Agent? Decision tree



# Why AI Agent projects fail?

# The risky business of AI

More than 80 percent
of AI projects fail.


**Twice the rate of failure
for information technology
projects that do not involve AI.**

Source: RAND | The Root Causes of Failure for Artificial Intelligence Projects and How They Can Succeed 2024

# The risky business of AI

70% of AI implementations led to abandonment due to integration challenges


Source: McKinsey's analysis of enterprise deployments

# **AI project** failure funnel

No clear and well-defined objectives

Shaky foundation: Poor-Quality Data

Talent Gaps and Poor Stakeholders involvement

Poor use case selection

Cutting-Edge Technology Over Practical Solutions

Unrealistic expectations & timelines

Inadequate Infrastructure for Deployment

Neglecting ethical and legal considerations

End users aren't ready

# A deeper look at pitfalls

# Unrealistic expectations (FOMO projects)

Common mistake

## Risk

- Stakeholders think “I have this **great idea** how GenAI can turn my business around”
- Little sceptical thinking **due to perceived first mover advantage**
- Unreasonably high and complex **expectations**

## Solution

- Run simple analysis, like **SWOT or TELOS** (technical, financial, market, operational, and legal)
- Focus on “boring” not “exciting” AI Agents
- Trust experienced partners to **assess the initial scope**

**3.2x**

**Projects with SMART goals show 3.2x higher success rates**

Source: MBS whitepaper “Why AI projects fail”

# Misaligned goals: setting AI projects up for failure

Common mistake

## Risks

- AI doesn't match **business needs** (e.g., expecting full automation when human input is needed).
- No clear **success metrics** → unclear project outcomes.
- Poor **stakeholder communication** → unrealistic expectations or incomplete requirements.

## Solutions

- **Run workshops** to align AI goals with business needs.
- Involve **key stakeholders** early in planning use cases
- Keep **communication open** between tech and business teams.

**38%** **projects failed due to deploying agents without validated business needs**

Source: MBS whitepaper "Why AI projects fail"

# Poor data foundations: garbage in, garbage out (GIGO problem)

Common mistake

## Risk

- **Poor-quality or incomplete data** → unreliable AI results.
- Problems with **accessing third party systems**
- Relying on primary data only, **without instructions, guardrails**

## Solution

- AI projects require **data strategy**
- **Conduct data audits** to find gaps, inconsistencies, or biases.
- Start with **simpler data**
- Continuously **monitor and clean** datasets to ensure relevance.

**60%** **project fail due to data issues, including poor quality and insufficient quantity**

Source: RAND | The Root Causes of Failure or Artificial Intelligence Projects and How They Can Succeed 2024

# Neglecting ethical and legal considerations

Common mistake

## Risk

- Non-diverse training data might lead to unintended but **serious consequences**
- security vulnerabilities
- misuse or exposure sensitive personal data if privacy laws and best practices are not followed.

**67%** **Americans express concerns about AI making biased or unfair decisions in hiring, lending, and policing**

Source: Pew Research 2023

## Solution

- Create **compliance frameworks** for data privacy and security (data encryptions, security testing, role-based access control)
- Curate **balanced** training data
- Embed **fairness metrics** in model evaluation
- Implement **continuous** bias testing post-deployment

# Trivial testing: Missing the real challenges

Common mistake

## Risk

- **Limited testing** → hidden errors go unnoticed.
- **Ignoring user feedback** → real issues remain unresolved.
- **Testing in ideal conditions** → poor real-world performance.

## Solution

- Test with **diverse edge cases** and stress scenarios.
- Actively **collect and apply** user feedback before scaling.
- **Expand pilot programs** gradually to ensure scalability.

**54%** **organizations report >$50M losses from poorly governed AI initiatives, particularly in regulated industries** “

source: Melbourne Business School whitepaper “ why do AI analytics and projects fail”

# Underestimation of complexity

Common mistake

## Risk

- Perceived ease of implementation: “configure OpenAI and connect to interface” is **not enough**
- GenAI projects are **real IT projects:** with analytics, data preparation, prevention of hallucinations, project management, testing

**85%**

**Projects fail due to underestimating complexity**

Source: Gartner

## Solution

- Create **compliance frameworks** for data privacy and security.
- **Balance** synthetic data with real-world data for training.
- Continuously **monitor and clean** datasets to ensure relevance.

# “Simple” product recommender task scope

1. Project Setup
2. Establish database schema and implementation
3. Data acquisition
4. Separation of the test dataset
5. Preparation of vector database and embeddings
6. Validation of recommendations
7. Building the Master Chat
8. Basic UI for ChatBot based on a ready-made template
9. Implementation of language security (Guardrails)
10. Bot logic
11. Implementation of the RAG head flow
12. Additional time for prompt engineering (testing and refinement)
13. Basic admin panel
14. Saving conversation history
15. The fallback mechanism for missing a potential response
16. Speech-2-text
17. Limiting conversation context
18. Support for tool calling and tool descriptor
19. Multi-language
20. Support for "tool calling" & chat tools descriptors
21. Simple questions scenarios (product info, brand comparison, shop info)
22. Project-based related tools (advice based on articles)

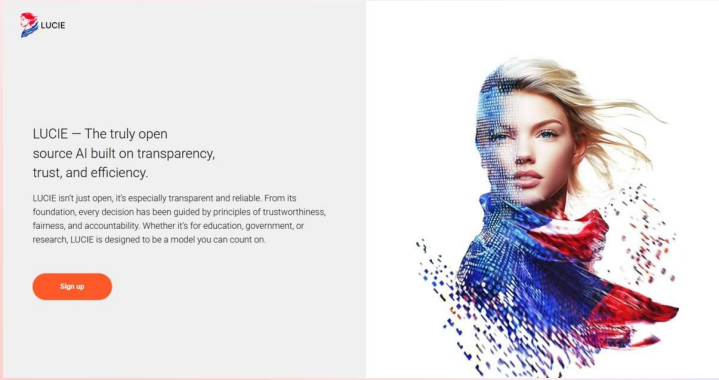
# Real-world failure examples

# The over-hyped chatbots

Case Study

## Real world example:

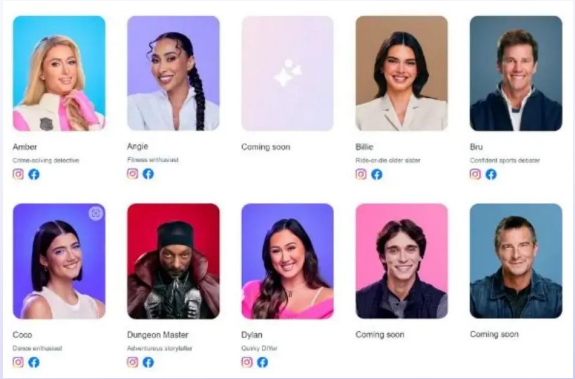
**The French AI chatbot 'Lucie' was launched with high expectations but faced suspension due to numerous errors and public criticism.**




Source: Le Figaro & lucie.chat

## Real world example:

**Meta's AI-powered celebrity chatbots were discontinued after user disinterest and negative feedback.**




Source: New York Post & Facebook

# The data starved AI tool

Case Study

Real world example:

Watson often recommended unsafe or impractical treatments.

**This was due to its reliance on limited, synthetic training data rather than real-world medical data. Additionally, it lacked integration with healthcare professionals' expertise.**

**$62M**

**loss**

**Consequence:** Produced dangerous treatment recommendations (e.g., bleeding medication for hemorrhaging patients)

Source:healtharkinsights.com/wp-content/uploads/2023/11/IBM-Watson-From-healthcare-canary-to-a-failed-prodigy

# The biased hiring tool

Case Study

Real world example:

**Amazon's AI recruitment tool exhibited bias against female candidates due to training on male-dominated resumes.**


**44%** of AI ethics incidents involve agentic systems rather than static models

# The human touch dilemma

Case Study

Real world example:

Forward's AI-powered 'CarePods'
aimed to revolutionize healthcare
but shut down in 2024 due to low patient adoption.

**Users resisted using the autonomous kiosks, citing discomfort with the technology and preference for human interaction.**


**$620M**
**investment failure**

**Consequence:** Despite plans to deploy 3,200 CarePods in 2024, Forward managed to launch only five before ceasing operations

# Proof of Concept or Proof-of-Collapse?

Case Study

Real world example:

**Zillow iBuying Algorithms**
**Property valuation models overestimated home prices during market shifts.**


**Consequence:**

**$881M** loss

**25%** workforce reduction

**EXIT** from home-flipping business

# Key Takeaways

- Work with **real agentic AI systems** and not just your off-the-shelf RAG if your customer experience is worth something to you
- Use **AI agents for adaptive, high-complexity tasks** --> traditional automation for repetitive workflows.
- ROI must align with both **financial and strategic** business goals.

Partner with experts for **technical** and **regulatory hurdles.**

# How to set yours for success

# 10 Top best-practices

1. Define **clear objectives** and scope for you AI agent
2. **Start small** with prototyping to identify risks early.
3. **Focus on data** for effective learning.
4. Choose the right development **tools and platforms** for scalability and efficiency.
5. Ensure matter experts  and internal **stakeholder involvement**
6. Adopt a **human-in-the-loop** approach for ongoing oversight and improvement.
7. Continuously **train and test** to avoid overfitting and ensure reliability.
8. Ensure seamless integration with existing systems using APIs.
9. Monitor and optimize performance using key metrics and alerts.
10. Prioritize ethics and user trust - **transparency is key**.

# Q&A

**Kara Herbut**

Sales Director · Services & Solutions

kara.herbut@deviniti.com

# Thank you

for your attention!

www.deviniti.com